Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Amendment of the Commission's Rules to	)	WT Docket No. 04-435
Facilitate the Use of Cellular Telephones and	)	
other Wireless Devices Aboard Airborne Aircraft	)	
In the Matter of	)	
	)	
Communications Assistance for	)	ET Docket No. 04-295
Law Enforcement Act and	)	
Broadband Access and Services	)	RM-10865

Comments of VeriSign, Inc.

Anthony M. Rutkowski
Vice President for Regulatory Affairs
VeriSign Communications Services Div.
21355 Ridgetop Circle
Dulles VA 20166-6503
tel: +1 703.948.4305
mailto:trutkowski@verisign.com

Brian Cute
Vice President, Government Relations
1666 K Street, N.W., Suite 410
Washington DC 20006-1227
tel: +1 202.973.6615
mailto:bcute@verisign.com

Michael Aisenberg
Director, Government Relations
1666 K Street, N.W., Suite 410
Washington DC 20006-1227
Tel: +1 202.973.6611
mailto:maisenberg@verisign.com

Raj Puri
Vice President, NetDiscovery Service
487 East Middlefield Road
Mountain View 94043-4047
tel: +1 650.996.2927
mailto:rpuri@verisign.com

Filed: 23 May 2005

EXECUTIVE SUMMARY

The Commission in this Notice of Proposed Rulemaking (NPRM) [1] is moving forward with enabling and facilitating the use of 800 MHz cellular and potentially other wireless handsets and devices on-board aircraft. This should benefit consumers by adding to future and existing air-ground communications options that will provide greater access for mobile voice and broadband services during flight.

The use of such devices and services does, however, raise significant concerns and challenges with respect to the effective implementation of network forensic and law enforcement assistance requirements including CALEA capabilities being considered in the context of an ongoing related proceeding.[2] These forensic and assistance requirements are essential not only for the protection and security of the on-board services, but also to mitigate and respond to the inevitable use of these services for criminal, terrorism, or other unlawful purposes. In addition to the technical challenges, there also exist significant jurisdictional and legal complexities associated with on-board law enforcement assistance capabilities that must be remedied in the implementing architectures. A panoply of diverse global aircraft, citizens, service providers, and applicable law are inherently involved.

The necessary on-board law enforcement assistance requirements can be efficiently and effectively supported for on-board communication providers today through the Trusted Third Party service bureau model proposed in the *CALEA NPRM*. This architecture, which VeriSign already offers to communication providers, has proven invaluable for providers and law enforcement, as well as the general public which must ultimately bear the risks, costs, and privacy burdens.

VeriSign urges the Commission to address analogous needs presented in a holistic manner in this On-board wireless proceeding. The required capabilities should go to facilitating the procedural, operational, and technical mechanisms for 1) rapid authenticated discovery of nomadic users and service providers, as well as 2) the ability upon proper authorization to produce stored or real-time traffic data and content for handover to law enforcement. Because of the substantial technical, operational, and jurisdictional challenges and complexities involved in meeting law enforcement assistance needs, the Commission should consider the exclusive use of accredited Trusted Third Party service bureaus for this purpose.

---

[1] *Amendment of the Commission's Rules to Facilitate the Use of Cellular Telephones and other Wireless Devices Aboard Airborne Aircraft*, WT Docket No. 04-435, Notice of Proposed Rulemaking, FCC 04-288 (15 Feb 2005), (hereinafter referred to as *On-board NPRM).*

[2] *See Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Notice of Proposed Rulemaking and Declaratory Ruling in the Matter of, ET Docket No. 04-295, RM-10865, Document 04-187 (9 Aug 2004), (hereafter referred to as *CALEA NPRM*).

1. For more than a decade, VeriSign has provided an array of large-scale, ultra-high availability, trusted infrastructures that enable signalling, security, identity management, directory, financial transaction, and fraud management capabilities for a broad array of network based business and consumer services – whether it be Internet, Web, Internet access, traditional voice telephony, VoIP, multimedia, next generation, or sales. VeriSign operates through various divisions that have offices and staff in the U.S. and worldwide. In these various capacities, it participates in scores of different forums, working collaboratively with both industry and government to find entrepreneurial oriented solutions.

2. As part of these commercial infrastructure support services, VeriSign provides as a Trusted Third Party both lawfully authorized electronic surveillance (lawful interception) capability requirements to communication providers globally, and other lawful access services (i.e., subpoena processing). It also participates in or leads many of the related technology, industry, and standards activities.

Facilitating use of wireless handsets on aircraft should encompass forensic and law enforcement needs

3. The Commission in this Notice of Proposed Rulemaking (NPRM) innovatively proceeds in moving forward with enabling and facilitating the use of 800 MHz cellular and potentially other wireless handsets and devices on-board aircraft. As noted in the *On-board NPRM* introduction, these actions "…should benefit consumers by adding to future and existing air-ground communications options that will provide greater access for mobile voice and broadband services during flight."[3] This action promises to make available a cornucopia of wireless Next Generation Network (NGN) services on board aircraft worldwide, and initial commercial implementations and regulatory actions have already occurred.[4]

---

[3] *On-board NPRM, supra* at para. 2.

[4] *See, e.g.*, ConneXion, http://www.connexionbyboeing.com/; Tenzing, http://www.tenzing.com; *Amendment of part 22 of the Commission's Rules to Benefit the Consumers of Air-Ground Telecommunications Services; Biennial Regulatory Review - Amendment of Parts 1,22, and 90 of the Commission's Rules*, WT Docket No. 03-103, Report and Order, FCC 04-287, (22 Feb 2005); Assignment of Country Code and Identification Code +882 98 to SITA, SITA GSM services in aircraft, +882 99 to Telenor, Telenor GSM network – services in aircraft, ITU-T, Telecommunication Standardization Sector of

4. Although the *On-board NPRM* states that this action "…would be consistent with the Commission's efforts to promote homeland security by increasing communications options available for public safety and homeland security personnel...," the NPRM fails either to address the communications forensic needs of law enforcement, focusing largely instead on spectrum management matters.[5] The use of such devices and services does, however, raise significant concerns and challenges with respect to the effective implementation of network forensic and law enforcement assistance requirements including capabilities being considered in the context of the *CALEA NPRM*, as well as existing CALEA statutory requirements implemented in the Commission's legacy 97-213 CALEA docket proceeding.

5. The on-board wireless services provisioning environment is by definition highly nomadic – both as to providers and subscribers. With a diverse multiplicity of domestic and international air carriers and aircraft constantly in motion, it will be inherently difficult to discover communications transport provider arrangements. Layered on top of the communications transport are an unlimited array of potential virtual providers of diverse services that may exist anywhere in the world. The subscriber usage will be even more transient as potentially millions of individuals gain access to the on-board services for a few minutes or hours using an array of diverse, essentially untraceable communications devices. The starting point for meeting both the spirit and the letter of CALEA is providing law enforcement with the ability to know through some reasonably effectively authenticated and rapid mechanism, 1) the identity and contact information for on-board communication service providers, and 2) the identity and contact information for on-board users of those services, including their communication service identifiers.

6. In addition to the technical challenges, there also exist significant potential jurisdictional and legal complexities associated with on-board law enforcement assistance capabilities that should be addressed in the implement architectures. Jurisdictional

---

ITU, *Complement to ITU-T Recommendation E.164 (02/2005), List of ITU-T Recommendation E.164 Assigned Country Codes (Position on 1 May 2005)* at 17; Asia-Pacific Telecommunity, *Working Document Towards a Proposed Framework on the Use of Mobile Phones on Board Aircraft*, The APT Wireless Forum Interim Meeting 2005, Doc. AWF-IM1/37(Rev.2) (4 Mar 2005) (hereafter cited as *APT Draft Framework*).

[5] *See id* at paras 10-25.

parameters include the flag of the carrier, and locations of the craft in airspace, of the communications service provider, and of the customer records or access point to real-time data or content. As the Commission noted in the *CALEA NPRM*, implementation architecture can make a dramatic difference in effective ability of capabilities and costs, and this difference is especially relevant to complex issues of jurisdiction and availability where on-board support to law enforcement is involved.[6]

The Commission has the necessary jurisdiction and authority to require assistance to law enforcement by on-board communication services providers

Production of Provider and Subscriber Identity Information

7. Law enforcement's concerns regarding assistance in identifying providers and subscribers has already been expressed to the Commission in conjunction with the availability of new technology.[7] This availability of subscriber or customer identity information to law enforcement as well as Trusted Third Party service bureaus that are faced with the task of implementing law enforcement orders. Knowledge of providers and subscribers is a critical precursor in any investigation and typically occurs either prior to obtaining a subpoena or intercept order, or during the course of collecting and analyzing stored or real-time traffic data. Almost all CALEA Sec. 103 capability and exclusion requirements, as well as Sec. 207 disclosure provisions, are fundamentally dependent on the expeditious availability of information that allows law enforcement to know if the provider serves a particular customer, as well as the "bindings" of that customer to communication identifiers (telephone number, IP address, etc) used for telecommunication or IP-Enabled services.

8. Providers of public telecommunication services have long been under diverse obligations to maintain authenticated customer or subscriber databases that are expeditiously accessible through standardized interfaces via the SS7 Intelligent Network

[6] *See CALEA NPRM* at paras 69-76, Appendix C.
[7] *See Comments of the Department of Homeland Security in the Matter of FCC Review of Regulatory Requirements for IP-Enabled Services*, WC Docket No. 04-36, filed 28 May 2004; *Comments of the United States Department of Justice in the Matter of IP-Enabled Services*, WC Docket No. 04-36, filed 28 May 2004. *See also*, Sec. 103, Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279.

infrastructure. Comparable capabilities are needed in conjunction with either broadband Internet access or managed/mediated VoIP services. Without the expeditious access to authenticated subscriber or customer information, other CALEA capabilities for the production of stored or real-time data or content are degraded at best and meaningless at the worst.

9. Another basis for such a database requirement goes to the Substantial Replacement and public interest provisions of the 1994 Act. Just as broadband Internet access and managed/mediated VoIP are the emerging Next Generation Network equivalent of circuit-switched telephone exchange telephony service, so too are NGN directory services the replacement of existing Intelligent Network subscriber and customer databases. To do otherwise would also unfairly discriminate against existing public telephony providers who typically take steps to authenticate customers and maintain accessible records via the Intelligent Network infrastructure.

10. Open standards-based NGN capabilities to discover and query provider and subscriber information are under development.[8] Action that requires this support capacity in the context of multiple CALEA capability requirements in this proceeding seems not only necessary, but critical to the very purpose of CALEA.

Production of Stored Data and Content

11. Availability and access to stored traffic data (i.e., call-identifying information) are especially significant operational and law enforcement forensics requirements for on-board communications, given the very transitory nature of the services, and the nomadic proclivities of the subscribers. In the United States, such requirements arise through the use of subpoenas or preservation orders. In many other countries, they may arise additionally through data retention regulations.

12. The Commission has Title I, II, and III authority in the context of on-board wireless services to provide for such requirements. In addition, CALEA section 103 also contemplates such capability requirements in conjunction with implementation of court

[8] *See, e.g., An NGN Directory Framework Overview - Supporting Critical Operational and Security Requirements*, ITU-T Doc. COM13-D133 (Apr 2005); VeriSign *ex parte* presentation in Docket No. 04-295, 2 Nov 2004. *See also, NECA notification to ATIS of IPES Company Code Category*, TMOC – ATIS Telecom Management and Operations Committee, TMOC-2005-029, 11 May 2005.

orders or other lawful authorization as ancillary to real-time access requirements. The CALEA Act requires that communication providers provide a capability of:

> (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier--
>
> > (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and
> >
> > (B) in a manner that allows it to be associated with the communication to which it pertains…
>
> (3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier;

Section 102 in turn defines "call-identifying information" as:

> (2) …dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.

In addition to CALEA statutory provisions, the Convention on Cybercrime explicitly includes capabilities for mutual assistance for access to subscriber information and stored computer data in exactly the same kind of complex transnational law enforcement support situations that can be expected in conjunction with on-board communications.[9]

13. As discussed above with respect to access to subscriber identity information for broadband Internet access and managed/mediated VoIP providers, the maintenance and rapid availability of stored traffic data is critical to law enforcement for investigative forensic and evidentiary purposes. Indeed, it is so important that the number of requests exceeds the number of real-time intercept orders by a factor of 10 to 50 times. As a long term trend - given the increasing nomadicity of users, the dispersion of providers, and the use of encrypted content – the rapid availability of stored traffic data is likely to increase in importance and quantity of production orders.

14. In the United States, service providers do not ordinarily get reimbursed for producing stored traffic data for criminal investigations and cases to law enforcement. Both anecdotal information and some comment in the early phase of the Commission's

[9] *See* Art. 31 - Mutual assistance regarding accessing of stored computer data, *Convention on Cybercrime*, Budapest, 23.XI.2001.

Docket 04-295 CALEA proceeding, made it clear that the production of stored traffic data is far more onerous and costly than CALEA support for most if not all service providers. This burden is likely to be significant for the providers of on-board communications services. As a result, there appears to be a significant confluence of interests by both service providers and law enforcement in developing a standard interface for "…delivering…[stored] call-identifying information to the government" pursuant to CALEA section 102(a)(3). Substantial initial industry standards based activity has already been undertaken toward this end - both for the receipt of orders and the production of data. [10]

Commission action in this proceeding to establish an explicit capability requirement for access to stored traffic data would significantly advance the implementation of a common production interface and thereby provide significantly reduced costs for service providers, and reduced delays for law enforcement.

Production of Real-time Communications Data and Content

15. The Commission has clear jurisdiction and authority under CALEA as well as the Communications Act as amended to impose real-time communications data and content production capability requirements on the providers of on-board communication service providers; and indeed, the requirements are already instituted under existing Part 22 and 24 Rules for legacy cellular and PCS services, and being augmented with requirements for new Next Generation wireless services in the CALEA NPRM for broadband Internet access and managed/mediated VoIP services. Industry CALEA standards for the legacy service capabilities presently exist, and considerable lawful interception standards activity for various kinds of broadband wireless access and VoIP are underway, including international public wireless LANs.[11] Internationally, the Asia

[10] *See, e.g.*, ETSI, *Telecommunications Security; Lawful Access; Stored Data Handover Interface (SDHI)*, TSI TR 10X XXX V0.0.1 (2005-06).

[11] *See, e.g.*, TIA TR-45, *Lawfully Authorized Electronic Surveillance*, SP-3-4465-UGR2-2; *Lawful Interception in the 3GPP Rel-7 architecture*, 3GPP TSG-SA3 LI Meeting #17, S3LI05_058r1, Sophia Antipolis, France (April 2005); 3GPP/ETSI, *Technical Specification, Universal Mobile Telecommunications System (UMTS), 3G security, Handover interface for Lawful Interception (LI)*, ETSI TS 133 108 V5.6.0 (2003-12); ETSI, *Technical Report, Lawful Interception (LI), Lawful Interception of public Wireless LAN Internet Access*, ETSI DTR LI-00014 V0.1.0 (2005-05); ATIS, T1.IPNA-YEAR, *American National Standard for Telecommunications WORKING DOCUMENT for Lawfully Authorized*

Pacific Telecommunity has already explicitly provided for national lawful interception requirements in its *Proposed Framework on the Use of Mobile Phones on Board Aircraft*.[12]

On-board CALEA requirements should be implemented in a manner to support on-board law enforcement personnel

16. A third general area of system utilization to be considered in this proceeding is the actual use of on-board wireless capabilities by properly authorized law enforcement personnel, including TSA air marshals, other in transit law enforcement personnel, or other properly equipped personnel being provided access during emergencies. Since the inception of the Government Emergency Telecommunications System (GETS), there have been repeated instances of communications service outage where access to the PSTN by properly authorized national security and law enforcement personnel was enabled solely because of their possession of GETS access authorization and coding. The communications experience of diverse emergency responders to the World Trade Center and Pentagon attacks in 2001 is recounted vividly in the 911 Commission Report[13] and anecdotal accounts of the important role of GETS access enabling officials to access the telephone network abound.[14]

17. The instant proceeding provides an opportunity for the Commission to articulate carrier responsibilities and necessary network elements to enable the utilization of available wireless service by official personnel onboard aircraft. Not only would such access provide an obvious alternative means of communications during an actual on-board emergency (whether of a security nature or one involving passenger health or safety) but it would also provide immediate communications access to essential personnel who might otherwise be without communications capability until landing. Indeed, an on-board GETS capability - coupled with the ability to use that capacity for setting up a preservation or communications interception order – could be enormously valuable in circumstances where extrinsic evidence might dictate such action.

Electronic Surveillance (LAES) for IP Network Access, PTSC-LAES-2005-003R2 (May 2005); ATIS, *LAES of NGN*, PTSC Issue Number S0021, assigned 14 Apr 2005.

[12] *See APT Draft Framework, supra*.

[13] *See The 911 Commission Report* < http://www.9-11commission.gov/report/911Report.pdf >

[14] Remarks of General Harry Radijke to Members of the President's NSTAC XXVIII, 12 May 2005.

18. The provision of on-board GETS access is entirely within the capacity of existing GETS service providers from among the commercial carrier community, and would, if authorized, be deployable as a feature of general on-board wireless service. The role of SS7 services in such a system is readily apparent. VeriSign, as a service provider, is prepared to provide a synoptic service overview upon request. It is VeriSign's view as the general boundaries of on-board wireless are defined the opportunity to integrate such a potentially life-saving capability should not be overlooked.

The exclusive use of accredited Trusted Third Party service bureaus should be considered for implementation of law enforcement assistance requirements for on-board communication services

19. In addition to considering law enforcement assistance requirements in the instant On-board NPRM, and correlating CALEA requirements with those being considered in the CALEA NPRM, it seems appropriate for the Commission to consider what additional, special requirements should be imposed for on-board communication service providers. In the CALEA NPRM, the Commission described at considerable length the invaluable architectures and efficiencies that Trusted Third Party service bureaus offer for both providers and law enforcement. In light of the enormous technical, operational, and jurisdictional complexities associated with supporting law enforcement assistance requirements for on-board communications, it seems entirely appropriate to use such service bureaus exclusively for such assistance. Furthermore, such service bureau implementations can be effectively integrated with GETS capabilities for on-board law enforcement personnel.

20. The service bureau architecture, which VeriSign already offers to communication providers, has proven invaluable for providers and law enforcement, as well as the general public which must ultimately bear the risks, costs, and privacy burdens. The available effective alternatives here are limited. Without service bureaus, both providers and law enforcement officials are faced with the Herculean task of maintaining and correlating – sometimes in near real-time – databases of authenticated nomadic subscribers on-board aircraft, their transiently assigned communication

identifiers such as phone numbers or IP addresses, and secure capabilities to produce or preserve stored and real-time traffic data and content in response to any of thousands of different government authorities submitting a lawful subpoena or order.

21. Some countries will likely elect to meet this challenge through the simple expedient of a national governmental service bureau performing the necessary functions. In the U.S., however, it seems unlikely that such a governmental solution is appropriate in light of the competitive private-sector alternatives that exist. Private-sector alternatives offer greater fiscal and legal transparency and accountability as well as responsiveness to the rapidly changing technology and provisioning marketplace. To the extent that government oversight is necessary, an accreditation process and/or contractual agreements can be used.